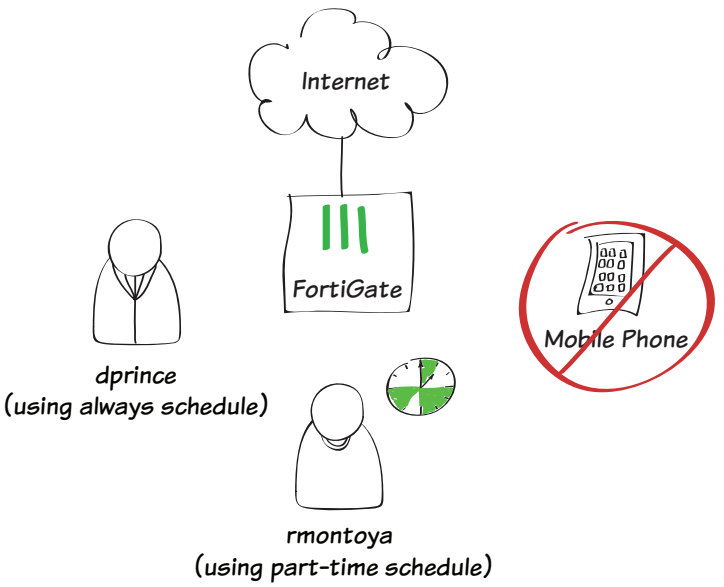
Allowing network access based on schedule and device type

In this example, user authentication and device authentication provide different access for staff members based on whether they are full-time or part-time employees, while denying all traffic from mobile phones.

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN.

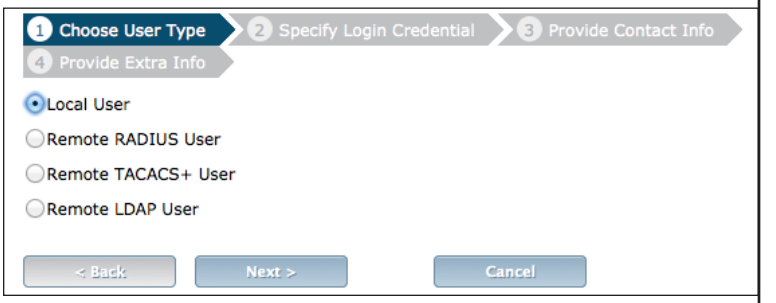
1. Defining two users and two user groups
2. Creating a schedule for part-time staff
3. Defining a device group for mobile phones
4. Creating a policy for full-time staff
5. Creating a policy for part-time staff that enforces the schedule
6. Creating a policy that denies mobile traffic
7. Results

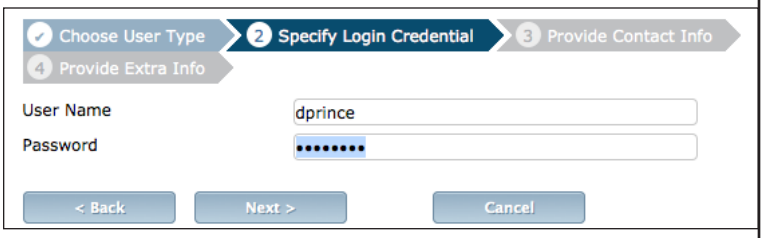


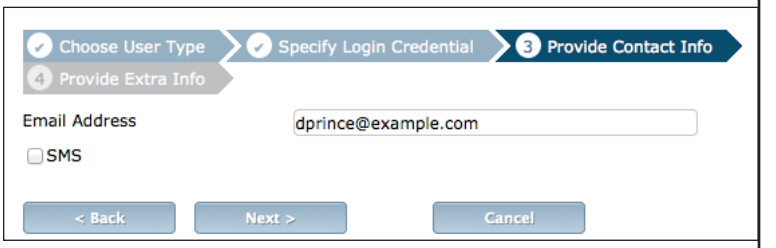
1. Defining two users and two user groups

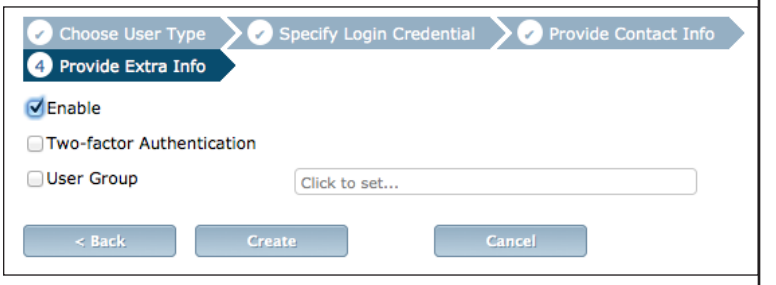
Go to **User & Device > User > User Definitions**.

Create two new users (in the example, *dprince* and *rmontoya*).







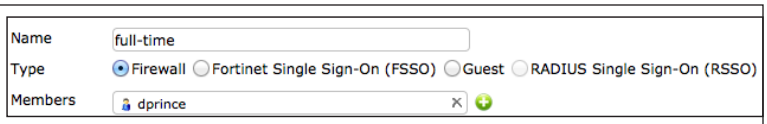


Both user definitions now appear in the user list.

User Name	Type	Two-factor Authentication	Ref.
dprince	LOCAL		0
guest	LOCAL		1
rmontoya	LOCAL		0

Go to **User & Device > User > User Groups**.

Create the user group *full-time* and add user *dprince.*

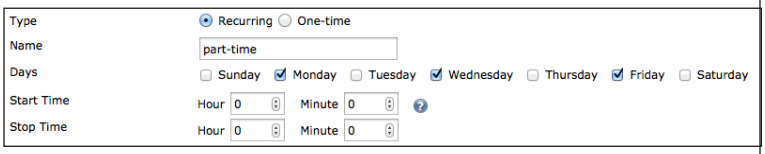


Create a second user group, *part-time*, and add user *rmontoya*.

2. Creating a schedule for part-time staff

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

Set an appropriate schedule. In order to get results later, do not select the current day of the week.



3. Defining a device group for mobile phones

Go to **User & Device > Device > Device Groups** and create a new group.

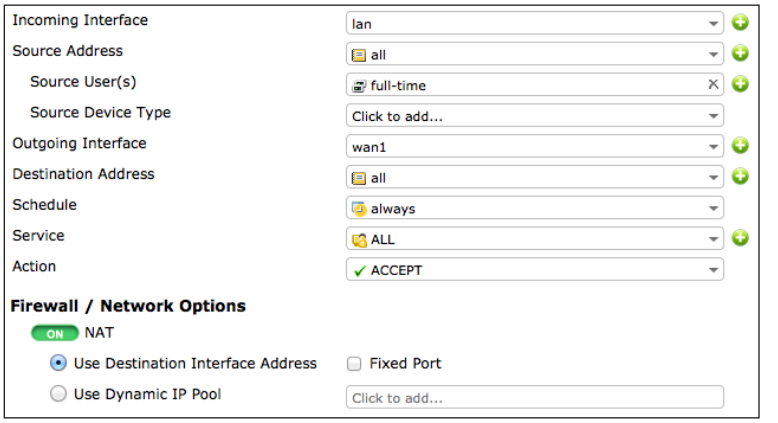
Add the various types of mobile phones as **Members**.

4. Creating a policy for full-time staff

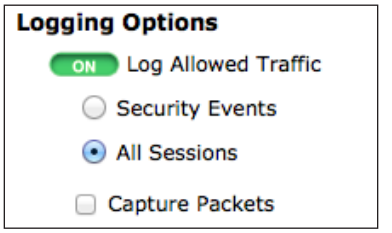
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the full-time group, **Outgoing Interface** to your Internet-facing interface, and ensure that **Schedule** is set to **always**.

Turn on **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

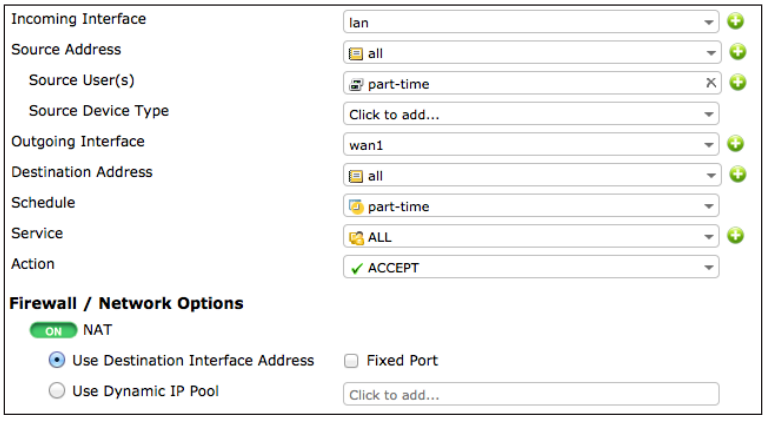


5. Creating a policy for part-time staff that enforces the schedule

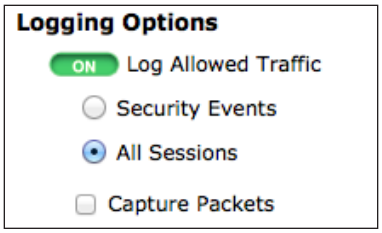
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the part-time group, **Outgoing Interface** to your Internet-facing interface, and set **Schedule** to use the part-time schedule.

Turn on **NAT**.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



View the policy list. Click on the title row and select **ID** from the dropdown menu, then select **Apply**. Take note of the ID number that has been given to the part-time policy.

Seq.#	From	To	Schedule	Source	Destination	ID
1	lan	wan1	always	all full-time	all	1
2	lan	wan1	part-time	all part-time	all	2
3	any	any	always	all	all	

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**, using the ID number of the part-time policy.

```
config firewall policy
   edit 2
      set schedule-timeout enable
   end
end
```

This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

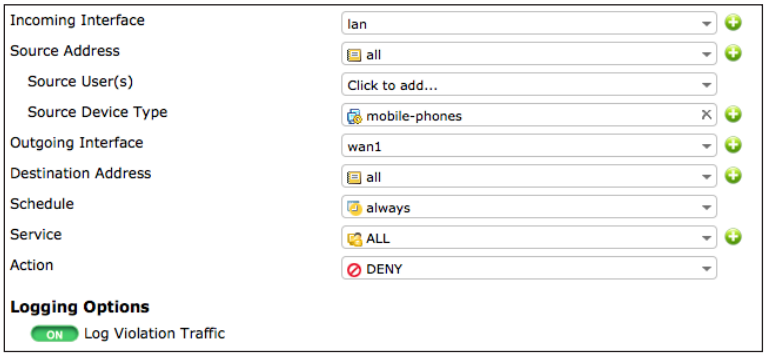
6. Creating a policy that denies mobile traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source Device** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and set **Action** to **DENY**.

Leave **Log Violation Traffic** turned on.

Using a device group will automatically enable device identification on the local network interface.



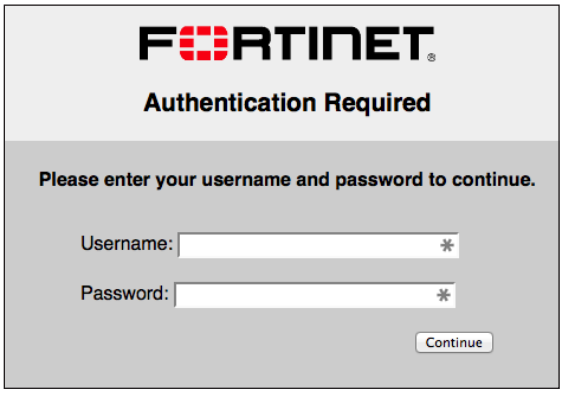
In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

Seq.#	From	To	Devices	Groups	Action
3	lan	wan1	Mobile Devices		DENY
1	lan	wan1		full-time	ACCEPT
2	lan	wan1		part-time	ACCEPT
4	any	any			DENY

7. Results

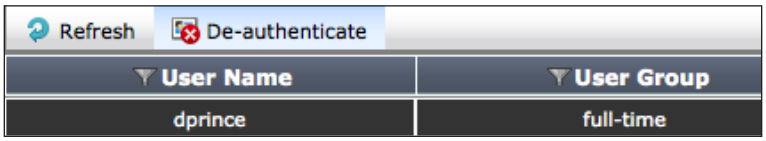
Browse the Internet using a computer. You will be prompted to enter authentication credentials.

Log in using the *dprince* account. You will be able to access the Internet at any time.



Go to **User & Device > Monitor > Firewall**. Highlight **dprince** and select **De-authenticate**.

Attempt to browse the Internet again. This time, log in using the *rmontoya* account. After authentication occurs, you will not be able to access the Internet.



Attempts to connect to the Internet using any mobile phone will also be denied.

You can view more information about the blocked and allowed sessions by going to **System > FortiView > All Sessions**.

Sessions that were blocked when you attempted to sign in using the *rmontoya* account will not have a user account shown in the **User** column.

Date/Time	User	Device	Destination	Action
09:10:21		iPhone	208.91.112.53	deny
09:10:21		Mac Mini	157.55.56.159	deny
09:10:21		Mac Mini	111.221.74.30	deny
09:10:21		Mac Mini	111.221.77.159	deny
09:10:21		iPhone	208.91.112.52	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:19		Mac Mini	157.55.56.159	deny
09:10:19		Mac Mini	157.56.52.30	deny
09:10:17		iPhone	208.91.112.52	deny
09:10:17	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:15	dprince	Mac Mini	64.94.107.34 (map-pb.quantserve.com.akadns.net)	accept
09:10:15	dprince	Mac Mini	174.36.240.82 (api.mixpanel.com)	accept